18

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/579,810 | 05/26/2000 | Victor Kouznetsov | 002.0132.01 | 7703 |

22895 7590 02/25/2005

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

| EXAMINER | |
|---|---|
| DADA, BEEMNET W | |
| **ART UNIT** | **PAPER NUMBER** |
| 2135 | |

DATE MAILED: 02/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/579,810 | KOUZNETSOV, VICTOR | |
| | Examiner | Art Unit | |
| | Beemnet W Dada | 2135 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *01 October 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. This office action is in reply to an amendment filed on October 01, 2004. Claims 1-21 are pending.

### *Claim Rejections - 35 USC § 103*

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 5-9, 13-17, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al (hereinafter Hill), US Patent 6,088,804, in view of Chen et al (hereinafter Chen), US Patent 5,960,170.

4. As per claims 1, 9, and 17, Hill discloses dynamically detecting computer viruses through associative behavioral analysis of runtime state (abstract), comprising: defining a group of monitored events which each comprise a set of one or more actions defined within an object (security events, col 7 ln 55-67 and col 8 ln 1-3), each action being performed by one or more applications executing within a defined computing environment (nodes, col 7 ln 55-67 and col 8 ln 13); continuously monitoring the runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group (continually respond, col 7 ln 55-67 and col 8 ln 1-3); tracking the sequence of the execution of the monitored events for each of the applications (first attack... number of security events, col 8 ln 22-35); identifying each

occurrence of a specific event sequence characteristic of computer virus behavior (comparing task, col 8 ln 3049); creating a histogram describing the specific event sequence occurrence for each of the applications (training signature into display map (col 7 ln 28-45); and identifying repetitions of the histogram associated with at least one object (comparing task, col 8 ln 30-49; also col 9 ln 8-25).

Hill further discloses identifying the location of a virus (location identifiers; col 45-59) and that such attacks can come from a plurality of locations, including applications (software, col 4 ln 35-41), wherein the virus detection occurs at a client computer (see for example; 26, fig 1 and col 4 ln 11-17). However, Hill et al does not explicitly teach identifying the application performing the specific event sequence. Chen discloses a means of virus detection wherein the application performing the specific event sequence (instructions) are identified (col 19 ln 39-67). Both Hill and Chen disclose a means of virus detection based on detecting events according to virus signatures. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Chen within the system of Hill because it would have increased simplicity by further identifying the application and thus provide more detailed information for the client or system to perform proper correction step.

In further regards to claim 1, Hill discloses a parameter set stored on a client system defining a group of monitored events (security agents ...located at nodes, col 4 ln 30-41) and a monitor executing on the client system (identify security events, col 4 ln 19-41) comprising a collector continuously monitoring the runtime state within the defined computing environment for an occurrence of any one of the monitored events in the group (col 4 ln 30-41; also task 82 col 7 ln 5467 and col 8 ln 1-3). Hill et al further discloses an analyzer (col 8 ln 5-29).

5. As per claims 5, 13, and 21, Hill-Chen discloses the claimed limitations as described above (see claim 1). Hill further discloses detecting suspect activities within each histogram (compares, col 8 In 30-49), each suspect activity comprising a set of known actions comprising a computer virus signature (training signature, col 7 In 46-54 and col 8 In 30-49).

6. As per claim 6 and14, Hill-Chen discloses the claimed limitations as described above (see claim 5). Hill discloses detecting viruses based on suspect activity (security events, abstract) being selected from a class of message transmissions, configuration area, security setting accesses and impersonations (see for example; col 4 In 30-31, col 5 In 45-65). However, Hill et al does not explicitly teach each suspect activity being selected from the class of actions comprising file accesses, program executions, configuration area accesses, security setting accesses, and impersonations. Chen discloses monitoring suspect activity being selected from the class comprising file accesses, program executions, configuration area accesses, and security setting accesses (col 11 In 45-col 12 In 11). Activities are events that can be monitored as a security event. One of ordinary skill at the time of the applicant's invention would have been able to additionally monitor activities from the class of file accesses, program executions, message transmissions, configuration area accesses, security setting accesses, and impersonations. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Chen within the system of Hill et al because it would have improved security through a more robust list of activities to be monitored.

7. As per claims 7 and 15, Hill-Chen discloses the claimed limitations as described above (see claim 6). Hill further discloses detecting viruses based on suspect activity (security events, abstract). Hill further discloses such suspect activity being selected from a class of message

transmissions, configuration area, security setting accesses and impersonations (see for example; col 4 ln 3031, col 5 ln 45-65). However, Hill et al does not explicitly teach each suspect activity being selected from a group comprising files accesses, program executions, direct disk accesses, media formatting operations, sending of electronic mail, system configuration area accesses, changes to security settings, impersonations, and system calls having the ability to monitor system input/output activities. Chen discloses monitoring such suspect activity (col 11 ln 45-col 12 ln 11). Activities are events that can be monitored as a security event. One of ordinary skill at the time of the applicant's invention would have been able to additionally monitor activities from the class of file accesses, program executions, message transmissions, configuration area accesses, security setting accesses, and impersonations. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Chen within the system of Hill et al because it would have improved security through a more robust list of activities to be monitored.

8. As per claims 8 and 16, Hill-Chen discloses the claimed limitations as described above (see claim 1). Hill further discloses monitoring computer viruses comprising at least one form of unauthorized content selected from the group comprising a computer virus application, a Trojan horse application, and a hoax application (col 5 ln 46-65).

9. Claims 2-4 and 10-12 and 18-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Hill et al (hereinafter Hill), US Patent 6,088,804, in view of Chen et al (hereinafter Chen), US Patent 5,960,170, and further in view of Vaidya, US Patent 6,279,113.

10. As per claims 2, 10, and 18, Hill-Chen discloses the claimed limitations as described above (see claim 1). Hill discloses organizing the histograms into plurality of records (fig 3; col 5 ln 26-65; and col 7 ln 27-54) ordered by object and monitored event (fig 3). Hill-Chen does not teach the records ordered by application. Vaidya discloses a system for detecting network intrusion (abstract) including a storage manager (database handler, col 5 ln 46-67) organizing a database of records ordered by application (network objects, col 5 ln 45-66 and col 6 ln 1-56). One of ordinary skill in the art at the time of the applicant's invention would have been able to order the database records by the application for which the record pertains to. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Vaidya within the combination of Hill-Chen because it would have increased efficiency of the virus detection by allowing the detection to be specific to the application.

11. As per claims 3, 11, and 19, Hill-Chen discloses the claimed limitations as described above (see claim 1). Hill et al further discloses maintaining a structured database in which the plurality of records is stored (col 5 ln 39-45); and storing a histogram for each such specific event sequence occurrence in one such database record (col 5 ln 39-45 and col 7 ln 27-45). The Hill-Chen combination does not teach storing the records identified by the application by which the specific event sequence was performed. Vaidya discloses a system for detecting network intrusion (abstract) including using a database of records ordered by application (network objects, col 5 ln 45-66 and col 6 ln 1-56). One of ordinary skill in the art at the time of the applicant's invention would have been able to order the database records by the application for which the record pertains to. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Vaidya within the Hill-Chen

combination because it would have increased efficiency of the virus detection by allowing the detection to be specific to the application.

12. As per claims 4, 12, and 20, Hill-Chen discloses the claimed limitations as described above (see claim 1). Hill further discloses configuring the structured database as an event log organized by each event in the group of monitored events (fig 3, security events and frequency, col 8 ln 30-50); and updating the database record storing each specific event sequence occurrence with a revised histogram as each such occurrence is identified (Security system is adapted, col 9 ln 34-45).

## *Response to Arguments*

13. Applicant's arguments filed October 01, 2004 have been fully considered but they are not persuasive. Applicant argues that the Hill and Chen patents, taken as a whole do not provide a suggestion, motivation or reason to combine, and one of ordinary skill in the art at the time the invention was made would not have a reason to combine a network attack response teachings of Hill with the computer virus detection teaching of Chen. Applicant further argues that Hill fails to teach dynamically identifying each occurrence of a specific event sequence characteristic of behavior of a computer virus and application which performed the specific event sequence.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some

teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Both Hill and Chen disclose a means of virus detection based on detecting events according to virus signatures. The teachings of Chen can be combined with the system of Hill because it would have increased simplicity by further identifying the application and thus provide more detailed information for the client or system to perform proper correction step [see for example, Chen, col 20, lines 1-5].

With respect to applicant argument that Hill does not teach dynamically identifying each occurrence of a specific event sequence characteristic of behavior of a computer virus and application which performed the specific event sequence. Examiner would point out that, Hill discloses dynamic security detection (col 4 in 31-32), which is able to detect, among other events, events related to a virus (col 5 In 58-62), and that the "network can change responses to the attack as the type of attack changes" (col 5 In 4-fi), thus dynamic detection. The examiner asserts that the combination of Hill and Chen teaches the claimed limitations as recited in the claims. Accordingly rejections for claims 1-21 are respectfully maintained.

## *Conclusion*

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

February 20, 2005

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100